UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA

LINDSEY HOWARD, individually and on behalf of all others similarly situated, Plaintiff, v. CITRIX SYSTEMS, INC., Defendant.	Case No.: **CLASS ACTION COMPLAINT** **Jury Trial Demanded**

CLASS ACTION COMPLAINT

Plaintiff, Lindsey Howard, individually and on behalf of all persons similarly situated (the "Class" or "Class Members"), brings this class action Complaint against Defendant, Citrix Systems, Inc. ("Citrix"), based upon personal knowledge with respect to herself and on information and belief derived from, among other things, investigation of counsel and review of public documents as to all other matters and alleges as follows:

NATURE OF THE CASE

1. Plaintiff brings this class action case against Defendant Citrix for its failures to secure and safeguard its current and former employees' (and in some cases beneficiaries and/or dependents of those employees) personal information, including names, Social Security numbers, financial information, and other personally identifiable information ("PII") (collectively "Personal Information"), which Citrix collected as a condition of employment, and for failing to provide

timely, accurate and adequate notice to Plaintiff and other Class members that their Personal Information had been stolen and precisely what types of information were stolen.

2. On March 8, 2019, Citrix disclosed that cyber criminals had gained access to the internal Citrix network.[1] At that time, Citrix disclosed only that "it appears that the hackers may have accessed and downloaded business documents. The specific documents that may have been accessed, however, are currently unknown." *Id.* Even at that early time, however, the "FBI ha[d] advised that the hackers likely used a tactic known as password spraying, a technique that exploits weak passwords. Once they gained a foothold with limited access, they worked to circumvent additional layers of security." *Id.* The cyber security event initially disclosed by Citrix on March 8, 2019 is referred to hereinafter as the "Data Breach."

3. Ultimately, in late April 2019, Citrix sent notice confirming that hackers had access to its network between October 13, 2018 and March 8, 2019, and that "they removed files from our systems, which may have included files containing information about our current and former employees and, in limited cases, information about beneficiaries and/or dependents." *See* Data Breach Notice Letter, attached as **Exhibit A**. The Notice Letter further acknowledged that the information taken included names, Social Security numbers, and financial information. *Id.*

4. This Personal Information was compromised due to Citrix's acts and omissions and its failure to properly protect the Personal Information of its current and former employees.

5. Citrix could have prevented this Data Breach simply by adopting industry-standard security protocols. Password spraying is a well-known and defensible intrusion tactic.

[1] See Citrix Blog, *Citrix Investigating Unauthorized Access To Internal Network* (Mar. 8, 2019), *available at* https://www.citrix.com/blogs/2019/03/08/citrix-investigating-unauthorized-access-to-internal-network/ (last visited May 23, 2019).

6. Moreover, data breaches at technology companies have been rampant in the last few years, including at Citrix itself, giving Citrix undeniable notice of its need to protect its systems and the Personal Information they contain. While many companies have responded to recent breaches by adopting technology that helps make systems more secure, Citrix did not.

7. In addition to Citrix's failure to prevent the Data Breach, Citrix also failed to detect the breach for nearly five months while hackers exfiltrated data from its networks.

8. The Data Breach was the inevitable result of Citrix's inadequate approach to data security and the protection of its employees' Personal Information that it collected during the course of its business. The deficiencies in Citrix's data security were so significant that the intrusion by the hackers remained undetected for months, and was only revealed to Citrix when it was informed by the FBI.

9. Citrix disregarded the rights of Plaintiff and Class members by intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure its data systems were protected, failing to disclose the material fact that it did not have adequate computer systems and security practices to safeguard Personal Information, failing to take available steps to prevent and stop the Data Breach from ever happening, and failing to monitor and detect the Data Breach on a timely basis.

10. As a result of the Data Breach, the Personal Information of Plaintiff and Class members has been exposed to criminals for misuse. The injuries suffered by Plaintiff and Class members as a direct result of the Data Breach include:

a. identity theft and fraud resulting from the theft of their Personal Information;

b. costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;

c. costs associated with purchasing credit monitoring, credit freezes, and identity theft protection services;

d. unauthorized charges and loss of use of and access to their financial account funds and costs associated with inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit;

e. lowered credit scores resulting from credit inquiries following fraudulent activities;

f. costs associated with time spent and the loss of productivity or the enjoyment of one's life from taking time to address and attempt to ameliorate, mitigate and deal with the actual and future consequences of the Data Breach, including discovering fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection services, imposing withdrawal and purchase limits on compromised accounts, and the stress, nuisance and annoyance of dealing with all issues resulting from the Data Breach;

g. the imminent and certainly impending injury flowing from potential fraud and identify theft posed by their Personal Information being placed in the hands of criminals and misused via sale on the Internet black market;

h. damages to and diminution in value of their Personal Information entrusted to Citrix for the sole purpose of working for Citrix; and

i. the loss of Plaintiff's and Class members' privacy.

11. The injuries to Plaintiff and Class members were directly and proximately caused by Citrix's failure to implement or maintain adequate data security measures for the Personal Information.

12. Further, Plaintiff retains a significant interest in ensuring that her Personal Information, which, while stolen, remains in the possession of Citrix, is protected from further breaches, and seeks to remedy the harms she has suffered on behalf of herself and similarly situated individuals whose Personal Information was stolen as a result of the Data Breach.

13. Plaintiff, on behalf of herself and similarly situated individuals, seeks to recover damages, equitable relief, including injunctive relief, to prevent a reoccurrence of the Data

Breach and resulting injury, restitution, disgorgement, reasonable costs and attorneys' fees, and all other remedies this Court deems proper.

JURISDICTION AND VENUE

14. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million exclusive of interest and costs. There are more than 100 putative class members. And, at least some members of the proposed Class have a different citizenship from Citrix.

15. This Court has jurisdiction over Citrix as maintains its corporate headquarters in this District. Defendant is authorized to and conducts business in this District and is subject to general personal jurisdiction in this state.

16. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events and omissions giving rise to this action occurred in this District, Citrix maintains its headquarters within this District, and Citrix has caused harm to Class members residing in this District.

PARTIES

17. Plaintiff Lindsey Howard is a resident and citizen of Coral Springs, Florida and former employee of Citrix.

18. Defendant Citrix is a Delaware corporation with its principal place of business located in Ft. Lauderdale, Florida.

19. Citrix provides "digital workspace, networking, and analytics solutions," most prominently "Application Virtualization and Virtual Desktop Infrastructure," "a fully-integrated, cloud-enabled app and desktop virtualization solution that gives customers

the flexibility to remotely deliver desktops and applications – from any cloud, on-premises datacenters or both." *See* Citrix 2018 Form 10-K at 4, attached hereto as **Exhibit B**.[2] Citrix's holdings include its wholly-owned "GoTo family of service offerings," which consists of "GoToMeeting, GoToWebinar, GoToTraining, GoToMyPC, GoToAssist, Grasshopper and OpenVoice . . . ." *Id.* at 3

20. Citrix employed some 8,200 employees as of December 31, 2018, and had net revenues of $2.9 billion in 2018. *Id.* at 11, 29.

STATEMENT OF FACTS

A. Citrix and Its Awareness of Data Security Risk

28. Citrix is a major technology company, specializing in "delivering digital workspace, networking, and analytics solutions that help customers drive innovation and be productive anytime, anywhere." Exhibit B at 4. Chief amongst its most well-known products and services is its Virtual Desktop solutions, which allow users to remotely access their desktops and applications from anywhere. *Id.*

29. In 2018, Citrix produced net revenue of nearly $3 billion, leased or subleased over 1.5 million square feet of space around the globe, and employed in excess of 8,000 people. *See* Exhibit B at 11, 27, 29.

30. Consistent with its position at the vanguard of technology companies, Citrix is well aware of the risks associated with failing to protect its information systems and the Personal Information contained therein. Specifically, Citrix's public filings state:

[2] Citrix Systems, Inc., 2019 Form 10-K, *available at*: https://d18rn0p25nwr6d.cloudfront.net/CIK-0000877890/5a296e8b-c25a-4a37-a5df-ceb29faed950.pdf (last visited May 23, 2019).

> ***Actual or perceived security vulnerabilities in our solutions and services or cyberattacks on our networks could have a material adverse impact on our business, results of operations and financial condition***.
>
> Use of our solutions and services may involve the transmission and/or storage of data, including in certain instances customers' business, financial and personal data. Thus, **maintaining the security of our solutions, computer networks and data storage resources is important** as security breaches could result in solution or service vulnerabilities and loss of and/or unauthorized access to confidential information. We aim to engineer secure solutions and services, enhance security and reliability features in our solutions and services, deploy security updates to address security vulnerabilities and seek to respond to known security incidents in sufficient time to minimize any potential adverse impact. We have in the past, and may in the future, discover vulnerabilities in our solutions or underlying technology, which could expose our operations and our customers to risk until such vulnerabilities are addressed. In addition, to the extent we are diverting our resources to address and mitigate these vulnerabilities, it may hinder our ability to deliver and support our solutions and customers in a timely manner.
>
> As a more general matter, **unauthorized parties may attempt to misappropriate or compromise our confidential information or that of third parties, create system disruptions, product or service vulnerabilities or cause shutdowns**. These perpetrators of cyberattacks also may be able to develop and deploy viruses, worms, malware and other malicious software programs that directly or indirectly attack our products, services or infrastructure (including third party cloud service providers -- such as Microsoft Azure and Amazon Web Services and Google Cloud Platform - upon which we rely). Because techniques used by these perpetrators to sabotage or obtain unauthorized access to our systems change frequently and generally are not recognized until long after being launched against a target, we may be unable to anticipate these techniques or to implement adequate preventative measures.

Exhibit B at 15 (second and third emphasis added).

36. Citrix was further aware of its need to attract and retain talented employees:

> Our success depends, in large part, on our ability to attract, engage, retain, and integrate qualified executives and other key employees throughout all areas of our business. Identifying, developing internally or hiring externally, training and retaining highly-skilled managerial, technical, sales and services, finance and marketing personnel are critical to our future, and competition for experienced employees can be intense. . . .

> Competition for qualified personnel in our industry is intense because of the limited number of people available with the necessary technical skills and understanding of solutions in our industry. The loss of services of any key personnel, the inability to retain and attract qualified personnel in the future or delays in hiring may harm our business and results of operations.

Exhibit B at 14-15.

37. Despite recognizing these information security risks, and acknowledgment of its crucial need to attract and retain qualified employees, Citrix failed to adequately secure its systems, placing the Personal Information of its employees at serious risk.

38. At all relevant times, Citrix was aware, or should have been aware, that the Personal Information it collected, maintained and stored in its systems is highly sensitive, susceptible to attack, and could be used for wrongful purposes by third parties, such as identity theft and fraud. Indeed, Citrix observed frequent public announcements of employee data breaches at technology companies, healthcare companies, retailers, and restaurant chains and knew that personal and financial information of the type stored by Citrix is highly coveted and a frequent target of hackers.

39. In fact, in the years prior to the Data Breach, Citrix itself has been a frequent target for hackers across the globe. For example, in January 2016, an "altruistic" Russian hacker known as "w0rm" – who is infamous for attacks on a number of high profile targets including CNET, Adobe and Bank of America – stated in a blog post that he was able to gain access to Citrix's content management system via an insecure password. From there, w0rm "was able to exploit a

series of security holes to gain access to the company's administrative system including the remote assistance system."[3]

40. Cyberint, a cyber-security intelligence company based in Israel, said it identified the hack in October 2015 and promptly tried to notify Citrix. According to Elad Ben-Meir, vice president of marketing at Cyberint, the company made repeated efforts to notify Citrix but received no response. In addition, the hacker w0rm tweeted Citrix with a link to its blog posting on October 25, 2015 and said it received no response.[4]

41. According to Ben-Meir, an analysis of w0rm's attack showed that it had gained access to all of Citrix's customers through the administrative system. This would have enabled an attacker potentially to bypass customers' security systems and upload malware undetected. "Citrix offer[s] a platform for remote assistance – [w0rm] could if he wanted to – but he didn't actually use it, but if he wanted to he could penetrate every endpoint of Citrix customers out there," said Ben-Meir. "Essentially if he had wanted to, he could have put malware into every end user of every Citrix customer which then would allow it to either keylog the things the people type, he could steal sensitive information from those end points, or he could use those endpoints as a botnet to run DDos attacks. A hacker that gains access to that amount of PCs is basically really powerful." [5]

---

[3] Tom Reeve, *I hacked Citrix, says Russian hacker w0rm,* SC Magazine UK (Jan. 11, 2016), *available at*: https://www.scmagazineuk.com/i-hacked-citrix-says-russian-hacker-w0rm/article/1477764 (last visited May 23, 2019).

[4] *Id*.

[5] *Id*.

42. W0rm told media outlets that its goals were actually altruistic, and that the hack was driven by a desire to upgrade internet security. "By targeting high-profile sites, the group says it can raise awareness about security flaws."[6]

43. In response to the report, Citrix's Chief Security Officer Stan Black issued a statement acknowledging that while Citrix's content management system was accessed, the "server under question did not contain any customer, employee or other sensitive or confidential information."[7] The statement further noted that "**we have no evidence that this threat actor has accessed systems other than the single content management server.** We will continue to monitor the environment for unauthorized access and changes."[8]

44. In June 2016, GoToMyPC, a popular remote desktop software owned by Citrix that allows users to access computers remotely using a web browser, required all users to reset their passwords after disclosing it was "targeted by a very sophisticated password attack." A Citrix representative stated that "the recent incident was a password re-use attack, where attackers used usernames and passwords leaked from other websites to access the accounts of GoToMyPC users. At this time, the response includes a mandatory password reset for all GoToMyPC users.

---

[6] Alasdair Gilchrist, *W0rm hackers hit Citrix in show of power*, ITProPortal (Jan. 12, 2016), *available at*: https://www.itproportal.com/2016/01/12/w0rm-hackers-hit-citrix-show-power/ (last visited May 23, 2019).

[7] Stan Black, *No Access to Sensitive Info; No Broad Network Access*, Citrix.com (Jan. 18, 2016), *available at*: https://www.citrix.com/blogs/2016/01/12/no-access-to-sensitive-info-no-broad-network-access-4/ (last visited May 23, 2019).

[8] *Id*.

Citrix encourages customers to visit the GoToMyPC status page to learn about enabling two-step verification, and to use strong passwords in order to keep accounts as safe as possible."[9]

45. In December 2018, Citrix forced a password for users of its secure file sharing and transfer service known as Sharefile. In response to questions of whether Citrix or Sharefile had been breached, Citrix posted a blog post touting the importance of data security in a world of a "staggering" number of data breaches:

> 2018 has seen an unprecedented number of records breached by hackers. According to the Breach Level Index, in just the first half of 2018, more records were compromised than in all of 2017. The number of records compromised in 2018 is in the multi billions. It's staggering.
>
> With the credentials harvested from these attacks, and the bad guys knowing that people will use the same password for multiple systems and websites, "credential stuffing" — a type of cyber-attack where stolen emails and passwords obtained through these types of breaches are used to try and gain unauthorized access to other systems — has become a serious threat facing businesses and individuals.
>
> Late last week, not long after new high profile security breaches were revealed, in the course of our ongoing security monitoring, we saw incidences in ShareFile that had some of the characteristics of credential stuffing. After further analysis, we became very concerned that indeed perpetrators were using credentials obtained from breaches unrelated to ShareFile to attempt to gain access to individual accounts.
>
> We made an immediate decision to limit the risk to our ShareFile customers by forcing a password reset. We knew the timing over the weekend was not ideal, but felt it far more important to help our customers by fundamentally stopping the credential stuffing effort. We acknowledge it has been inconvenient to customers, and regret the inconvenience, but we were acting in our customers' best interests.

[9] Brian Krebs, *Citing Attack, GoToMyPC Resets All Passwords*, KrebsOnSecurity (June 20, 2016), *available at*: https://krebsonsecurity.com/2016/06/citing-attack-gotomypc-resets-all-passwords/ (last visited May 23, 2019).

> It was the most expeditious way to end the attack, and proactively help our customer protect their data.[10]

46. But despite Citrix's stated desire to protect its *customer* information, it failed to implement reasonable safeguards to protect its own *employees'* information maintained by the company. As Citrix recognized, Personal Information is a valuable commodity on underground markets because it contains not only financial information but other PII as well. A "cyber blackmarket" exists in which criminals openly post stolen payment card numbers, financial account numbers, Social Security numbers, and other personal information on multiple underground Internet websites. Personal Information is valuable to identity thieves because they can use victims' personal data to open new financial accounts and take out loans in another person's name, incur charges on existing accounts, or clone ATM, debit, or credit cards.

47. Citrix, by employing individuals in its business operations, including Plaintiff and Class Members, obtained and retained the Personal Information of Plaintiff and Class Members. This personal and financial information is not otherwise available to the public, due to its private and confidential nature.

48. Legitimate organizations and the criminal underground alike recognize the value of PII contained in a merchant's data systems; otherwise, they would not aggressively seek or pay for it. At all relevant times, Citrix knew, or reasonably should have known, of the importance of safeguarding Personal Information and of the foreseeable consequences that would occur if its

[10] Stan Black, *Citrix forces password reset to protect against credential stuffing*, Citrix.com (Dec. 7, 2018), *available at*: https://www.citrix.com/blogs/2018/12/04/citrix-forces-password-reset-to-protect-against-credential-stuffing/ (last visited May 23, 2019).

data security system was breached, including, specifically, the significant costs that would be imposed on its customers as a result of a breach.

49. Citrix was, or should have been, fully aware of the significant volume of current and former employee information it retained, and thus, the significant number of individuals who would be harmed by a breach of Citrix's systems.

50. Unfortunately, and as alleged below, despite all of this publicly available knowledge of the continued compromises of Personal Information in the hands of other third parties, Citrix's approach to maintaining the privacy and security of the Personal Information of Plaintiff and Class members was lackadaisical, cavalier, reckless, or at the very least, negligent.

B. The Data Breach and Password Spraying

51. In its March 8, 2019 public announcement, Citrix disclosed that it had been contacted by the FBI and advised that "they had reason to believe that international cyber criminals gained access to the internal Citrix network."[11] Even at that early time, however, the "FBI ha[d] advised that the hackers likely used a tactic known as password spraying, a technique that exploits weak passwords. Once they gained a foothold with limited access, they worked to circumvent additional layers of security." *Id*.

52. On April 4, 2019, Citrix revealed additional information, noting that:

> We are devoting significant resources to manage this incident with painstaking deliberateness and thoroughness. We have brought on board multiple leading cyber security firms to assist our internal team with the work, and we continue to be engaged with the FBI.
>
> Based on where we are in the investigation at this point:

[11] Stan Black, *Citrix investigating unauthorized access to internal network*, Citrix.com (Mar. 8, 2019), *available at*: https://www.citrix.com/blogs/2019/03/08/citrix-investigating-unauthorized-access-to-internal-network/ (last visited May 23, 2019).

- We identified password spraying, a technique that exploits weak passwords, as the likely method by which the threat actors entered our network.
- We have taken measures to expel the threat actors from our systems. Additionally, we've performed a forced password reset throughout the Citrix corporate network and improved internal password management protocols.
- We have found no indication that the threat actors discovered and exploited any vulnerabilities in our products or services to gain entry.
- Based upon the investigation to date, there is no indication that the security of any Citrix product or service was compromised by the threat actors.[12]

53. Citrix ultimately notified Plaintiff and Class Members of the Data Breach by letter dated April 29, 2019. *See* **Exhibit A**. The letter confirmed that hackers had not only accessed Citrix's network between October 13, 2018 and March 8, 2019, but also "removed files from [Citrix's] systems, which may have included filed containing information about our current and former employees and, in limited cases, information about beneficiaries and/or dependents." *See* **Exhibit A**. The Notice Letter acknowledged that the stolen information could have included names, Social Security numbers, and financial information for current and former employees, including potentially their dependents and beneficiaries. *Id*.

54. The Notice Letter recommended that affected individuals "remain vigilant for incidents of fraud and identity theft by, for example, regularly reviewing your account statements and regularly monitoring your credit reports. If you discovery any suspicious or unusual activity on your accounts or suspect identity theft or fraud, be sure to report it immediately to your financial institutions." *Id*.

[12] Eric Armstrong, *Citrix provides update on unauthorized internal network access*, Citrix.com (Apr. 4, 2019), available at: https://www.citrix.com/blogs/2019/04/04/citrix-provides-update-on-unauthorized-internal-network-access/ (last visited May 23, 2019).

55. Unfortunately, Citrix's notification to affected individual was severely deficient in numerous respects. First, Citrix failed to disclose exactly who was affected and what information was compromised, instead using vague phrasing "information relating to certain individuals who are current and former employees, as well as certain beneficiaries and dependents" and giving non-exhaustive examples including "names, Social Security numbers, and financial information." But employers like Citrix routinely store all sorts of employee information, including full names and addresses, e-mail addresses, employee system passwords, tax information, W-2 and other IRS forms, insurance information that may include the personal information of dependents and family members, and payroll records, among others.

56. Affected individuals may take different protections depending on what information is at issue, for example contacting the IRS if the breach included W-2 or tax information, contacting their bank if financial account information was compromised, and/or contacting credit reporting agencies if Social Security numbers or other PII was stolen. By failing to identify exactly who was affected or what information was compromised, Citrix is preventing its current and former employees from taking meaningful, proactive, and targeted mitigation measures that could help protect them from years of financial headache and harm.

57. Moreover, the Data Breach was entirely preventable given that password spraying is a well-known tactic of cyber attackers. As explained by the Department of Homeland Security ("DHS") in a March 2018 alert:

> In a traditional brute-force attack, a malicious actor attempts to gain unauthorized access to a single account by guessing the password. This can quickly result in a targeted account getting locked-out, as commonly used account-lockout policies allow three to five bad attempts during a set period of time. During a password-spray attack (also known as the "low-and-slow" method), the malicious actor attempts a single password against many accounts before moving on to attempt a

> second password, and so on. This technique allows the actor to remain undetected by avoiding rapid or frequent account lockouts.
>
> Password spray campaigns typically target single sign-on (SSO) and cloud-based applications utilizing federated authentication protocols. An actor may target this specific protocol because federated authentication can help mask malicious traffic. Additionally, by targeting SSO applications, malicious actors hope to maximize access to intellectual property during a successful compromise.
>
> Email applications are also targeted. In those instances, malicious actors would have the ability to utilize inbox synchronization to (1) obtain unauthorized access to the organization's email directly from the cloud, (2) subsequently download user mail to locally stored email files, (3) identify the entire company's email address list, and/or (4) surreptitiously implements inbox rules for the forwarding of sent and received messages.[13]

58. DHS also described the typical "tactics, techniques, and procedures (TTPs)" of a password-spray attack, which include:

- Using social engineering tactics to perform online research (i.e., Google search, LinkedIn, etc.) to identify target organizations and specific user accounts for initial password spray
- Using easy-to-guess passwords (e.g., "Winter2018", "Password123!") and publicly available tools, execute a password spray attack against targeted accounts by utilizing the identified SSO or web-based application and federated authentication method
- Leveraging the initial group of compromised accounts, downloading the Global Address List (GAL) from a target's email client, and performing a larger password spray against legitimate accounts; and
- Using the compromised access, attempting to expand laterally (e.g., via Remote Desktop Protocol) within the network, and performing mass data exfiltration using File Transfer Protocol tools such as FileZilla.[14]

59. DHS also detailed the indicators of a password spray attack, which include:

---

[13] U.S. Dep't of Homeland Security, *Alert (TA18-086A): Brute Force Attacks Conducted by Cyber Actors* (Mar. 27, 2018, last revised March 28, 2018), *available at*: https://www.us-cert.gov/ncas/alerts/TA18-086A (last visited May 23, 2019).

[14] *Id*.

- A massive spike in attempted logons against the enterprise SSO portal or web-based application;
- Using automated tools, malicious actors attempt thousands of logons, in rapid succession, against multiple user accounts at a victim enterprise, originating from a single IP address and computer (e.g., a common User Agent String).
- Attacks have been seen to run for over two hours.
- Employee logons from IP addresses resolving to locations inconsistent with their normal locations.[15]

60. Importantly, *months before* the initial intrusion at Citrix began, DHS detailed both the typical victim environment for password spray attacks, and the methods to prevent such an intrusion:

> **Typical Victim Environment**
>
> The vast majority of known password spray victims share some of the following characteristics:
>
> - Use SSO or web-based applications with federated authentication method
> - Lack multifactor authentication (MFA)
> - Allow easy-to-guess passwords (e.g., "Winter2018", "Password123!")
> - Use inbox synchronization, allowing email to be pulled from cloud environments to remote devices
> - Allow email forwarding to be setup at the user level
> - Limited logging setup creating difficulty during post-event investigations
>
> …
>
> **Solution**

[15] *Id*.

Recommended Mitigations

To help deter this style of attack, the following steps should be taken:

- Enable MFA and review MFA settings to ensure coverage over all active, internet facing protocols.
- Review password policies to ensure they align with the latest NIST guidelines and deter the use of easy-to-guess passwords.
- Review IT helpdesk password management related to initial passwords, password resets for user lockouts, and shared accounts. IT helpdesk password procedures may not align to company policy, creating an exploitable security gap.
- Many companies offer additional assistance and tools [that] can help detect and prevent password spray attacks, such as the Microsoft blog released on March 5, 2018.[16]

61. In addition to lacking the necessary safeguards to secure data such as employee records containing financial information and Social Security numbers, Citrix did not have adequate monitoring systems and controls in place to detect the unauthorized infiltration after it occurred. Indeed, Citrix, like any company its size storing valuable data, should have had robust protections in place to detect and terminate a successful intrusion long before access and exfiltration could expand to thousands of employee files. In this case, Citrix only learned of the breach after the FBI warned Citrix its systems were compromised months after the fact.

C. Plaintiff's Employment with Citrix and Discovery of Breach

62. Plaintiff was hired by Citrix as a contractor in early 2006 and served in that role until approximately August 2007. From August 2007 through May 2018, Plaintiff was a full time employee of Citrix who held roles as a billing maintenance representative, consulting services

[16] *Id.* (footnotes omitted).

billing associate, and accounts receivable representative, among others. Plaintiff resigned from Citrix in May 2018 to pursue other opportunities.

63. As a condition of her employment, Plaintiff provided Citrix with significant amounts of her personal and financial information, including her name and address, Social Security number, bank and financial account information, insurance information, and payroll and tax information. Plaintiff also provided Citrix with personal information relating to her spouse and three minor children who were beneficiaries and dependents of Plaintiff.

64. After receiving the Notice Letter dated April 29, 2019, Plaintiff became fearful for the safety of herself and her family. As recommended by Citrix, Plaintiff has taken and continues to take steps to mitigate against possible harm, including daily monitoring of her and her family's credit reports, financial accounts, and paying a monthly fee to enroll in identity theft protection and credit monitoring services through Complete ID to help discover and protect against instances of identity theft or fraud.

65. Plaintiff has also suffered stress and anxiety worrying about the safety and financial well-being of her family and three minor children.

D. Had Citrix heeded this advice, and implemented the solutions recommended by DHS—such as implementing MFA or strengthening password requirements—its employees', former employees', and their beneficiaries/dependents' Personal Information would not now be in the hands of cybercriminals.Citrix Failed to Comply With FTC Requirements

66. Federal and State governments have also established security standards and issued recommendations to temper data breaches and the resulting harm to individuals and financial institutions. The Federal Trade Commission ("FTC") has issued numerous guides for business

highlighting the importance of reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[17]

67. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and practices for business.[18] The guidelines note businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

68. The FTC recommends that companies limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[19]

69. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect Personal Information, treating the failure to employ reasonable

[17] Federal Trade Commission, *Start With Security* (June 2015), *available at*: https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited May 23, 2019).

[18] Federal Trade Commission, *Protecting Personal Information: A Guide for Business* (Oct. 2016), *available at*: https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited May 23, 2019).

[19] FTC, *Start With Security*, *supra* note 17.

and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

70. Citrix's failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential employee data constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

71. In this case, Citrix was at all times fully aware of its obligation to protect the Personal Information of Citrix's employees. Citrix was also aware of the significant repercussions if it failed to do so because Citrix collected data from thousands of employees and knew that this data, if hacked, would result in injury to its employees, including Plaintiff and Class members.

72. Despite understanding the consequences of inadequate data security, Citrix failed to comply with industry-standard requirements.

73. As a technology company, Citrix understood the risks and consequences of inadequate data security, but nevertheless operated network systems with outdated operating systems and software; failed to detect the hackers' presence, notice the massive amounts of data that were being exfiltrated from its databases, or take any steps to investigate the numerous other red flags that should have warned the company about what was happening.

E. The Citrix Data Breach Caused Harm and Will Result in Additional Fraud

74. Without detailed disclosure to Citrix's employees and others impacted, affected individuals including Plaintiff and Class members have been left exposed, unknowingly and

unwittingly, for months to continued misuse and ongoing risk of misuse of their Personal Information without being able to take necessary precautions to prevent imminent harm.

75. The ramifications of Citrix's failure to keep Plaintiff's and Class members' data secure are severe.

76. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 17 C.F.R § 248.201. The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person." *Id*.

77. Personal identifying information is a valuable commodity to identity thieves once the information has been compromised. As the FTC recognizes, once identity thieves have personal information, "they can drain your bank account, run up your credit cards, open new utility accounts, or get medical treatment on your health insurance."[20]

78. Identity thieves can use personal information, such as that of Plaintiff and Class members, which Citrix failed to keep secure, to perpetrate a variety of crimes that harm victims. For instance, identity thieves may commit various types of government fraud such as: immigration fraud; obtaining a driver's license or identification card in the victim's name but with another's picture; using the victim's information to obtain government benefits; or filing a fraudulent tax return using the victim's information to obtain a fraudulent refund.

79. Annual monetary losses from identity theft are in the billions of dollars. According to a Presidential Report on identity theft produced in 2007:

[20] Federal Trade Commission, *Warning Signs of Identity Theft* (May 2015), *available at*: https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft (last visited May 23, 2019).

> In addition to the losses that result when identity thieves fraudulently open accounts . . . individual victims often suffer indirect financial costs, including the costs incurred in both civil litigation initiated by creditors and in overcoming the many obstacles they face in obtaining or retaining credit. Victims of non-financial identity theft, for example, health-related or criminal record fraud, face other types of harm and frustration.
>
> In addition to out-of-pocket expenses that can reach thousands of dollars for the victims of new account identity theft, and the emotional toll identity theft can take, some victims have to spend what can be a considerable amount of time to repair the damage caused by the identity thieves. Victims of new account identity theft, for example, must correct fraudulent information in their credit reports and monitor their reports for future inaccuracies, close existing bank accounts and open new ones, and dispute charges with individual creditors.[21]

80. The unauthorized disclosure of Social Security Numbers can be particularly damaging because Social Security Numbers cannot easily be replaced. In order to obtain a new number, a person must prove, among other things, he or she continues to be disadvantaged by the misuse. Thus, under current rules, no new number can be obtained until the damage has been done. Furthermore, as the Social Security Administration warns:

> A new number probably will not solve all your problems. This is because other governmental agencies (such as the Internal Revenue Service and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) likely will have records under your old number. Also, because credit reporting companies use the number, along with other Personal Information, to identify your credit record, using a new number will not guarantee you a fresh start. This is especially true if your other Personal Information, such as your name and address, remains the same.
>
> If you receive a new Social Security Number, you will not be able to use the old number anymore.

[21] Federal Trade Commission, *Combating Identity Theft A Strategic Plan* (April 2007), *available at*: https://www.ftc.gov/sites/default/files/documents/reports/combating-identity-theft-strategic-plan/strategicplan.pdf (last visited May 23, 2019).

> For some victims of identity theft, a new number actually creates new problems. If the old credit card information is not associated with the new number, the absence of any credit history under the new number may make it more difficult for you to get credit.[22]

81. Personal Information such as that stolen in Data Breach is highly coveted by, and a frequent target of, hackers.

- Thieves use the credit card information to create fake credit cards that can be swiped and used to make purchases as if they were the real credit cards;
- Thieves reproduce stolen debit cards and use them to withdraw cash from ATMs;
- Thieves can use the victim's Personal Information to commit immigration fraud, obtain a driver's license or identification card in the victim's name but with another's picture, use the victim's information to obtain government benefits, or file a fraudulent tax return using the victim's information to obtain a fraudulent refund; or get medical services using consumers' stolen information or commit any number of other frauds, such as obtaining a job, procuring housing, or even giving false information to police during an arrest.

82. In fact, Javelin Strategy and Research reports that identity thieves have stolen $112 billion in the past six years.[23]

83. Furthermore, reimbursing a consumer for a financial loss due to fraud does not make that individual whole again. On the contrary, identity theft victims must spend numerous hours and their own money repairing the impact to their credit. After conducting a study, the Department of Justice's Bureau of Justice Statistics ("BJS") found that identity theft victims

[22] Social Security Administration, *Identity Theft and Your Social Security Number* (June 2017), *available at*: http://www.ssa.gov/pubs/10064.html (last visited May 23, 2019).

[23] Javelin Research, *2016 Identity Fraud: Fraud Hits an Inflection Point* (Feb. 2, 2016), *available at:* https://www.javelinstrategy.com/coverage-area/2016-identity-fraud-fraud-hits-inflection-point (last visited May 23, 2019).

"reported spending an average of about 7 hours clearing up the issues" and resolving the consequences of fraud in 2014.[24]

84. There may be a time lag between when harm occurs versus when it is discovered, and also between when Personal Information is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[25]

85. Thus, Plaintiff and Class members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent credit and debit card charges incurred by them and the resulting loss of use of their credit and access to funds, whether or not such charges are ultimately reimbursed by the credit card companies.

F. Plaintiff and Class Members Suffered Damages

86. The Personal Information of Plaintiff and Class members is private and sensitive in nature and was left inadequately protected by Citrix. Citrix did not obtain Plaintiff's and Class members' consent to disclose their Personal Information to any other person as required by applicable law and industry standards.

---

[24] U.S. Department of Justice, *Victims of Identity Theft, 2014* (Sept. 2015) *available at*: http://www.bjs.gov/content/pub/pdf/vit14.pdf (last visited May 23, 2019).

[25] U.S. Government Accountability Office, *Report to Congressional Requesters* (June 2007), *available at*: http://www.gao.gov/new.items/d07737.pdf (last visited May 23, 2019).

87. The Data Breach was a direct and proximate result of Citrix's failure to properly safeguard and protect Plaintiff's and Class members' Personal Information from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices, and the common law, including Citrix's failure to establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiff's and Class members' Personal Information to protect against reasonably foreseeable threats to the security or integrity of such information.

88. Citrix had the resources to prevent a breach. Citrix made significant expenditures to market its products and tout its prowess in the technology field, but neglected to adequately invest in data security, despite the growing number of intrusions and several years of well-publicized data breaches.

89. Had Citrix remedied the deficiencies in its systems, followed DHS guidelines, and adopted security measures recommended by experts in the field, Citrix would have prevented or discovered the intrusion into its network and systems and, ultimately, the theft of its current and former employees' Personal Information.

90. As a direct and proximate result of Citrix's wrongful actions and inaction and the resulting Data Breach, Plaintiff and Class members have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and identity fraud, requiring them to take the time which they otherwise would have dedicated to other life demands such as work and effort to mitigate the actual and potential impact of the Data Breach on their lives including, inter alia, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial

institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports.

91. Citrix's wrongful actions and inaction directly and proximately caused the theft and dissemination into the public domain of Plaintiff's and Class members' Personal Information, causing them to suffer, and continue to suffer, economic damages and other actual harm for which they are entitled to compensation, including:

a. identity theft and fraud resulting from the theft of their Personal Information;

b. costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;

c. costs associated with purchasing credit monitoring, credit freezes, and identity theft protection services;

d. unauthorized charges and loss of use of and access to their financial account funds and costs associated with inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit;

e. lowered credit scores resulting from credit inquiries following fraudulent activities;

f. costs associated with time spent and the loss of productivity or the enjoyment of one's life from taking time to address and attempt to ameliorate, mitigate and deal with the actual and future consequences of the Data Breach, including discovering fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection services, imposing withdrawal and purchase limits on compromised accounts, and the stress, nuisance and annoyance of dealing with all issues resulting from the Data Breach;

g. the imminent and certainly impending injury flowing from potential fraud and identify theft posed by their Personal Information being placed in the hands of criminals and misused via sale on the Internet black market;

h. damages to and diminution in value of their Personal Information entrusted to Citrix for the sole purpose of working for Citrix; and

i. the loss of Plaintiff's and Class members' privacy.

92. Citrix continues to hold Personal Information of its current and former employees, including Plaintiff and Class members. Particularly because Citrix has demonstrated an inability to prevent a breach or stop it from continuing even after being detected, Plaintiff and members of the Class have an undeniable interest in ensuring that their Personal Information is secure, remains secure, is properly and promptly destroyed and is not subject to further theft.

CLASS ALLEGATIONS

93. Plaintiff seeks relief on behalf of herself and as a representative of all others who are similarly situated. Pursuant to Rule 23(a), (b)(2), (b)(3) and (c)(4), Fed. R.Civ. P., Plaintiff seeks certification of a Nationwide class defined as follows:

> All individuals residing in the United States whose Personal Information was compromised in the data breach initially disclosed by Citrix in or about March 2019 (the "Class" or "Nationwide Class").

94. Pursuant to Rule 23, and in the alternative to claims asserted on behalf of the Nationwide Class, Plaintiff asserts claims under the law of Florida on behalf of separate statewide classes, defined as follows:

> All individuals whose Personal Information was compromised in the data breach initially disclosed by Citrix in or about March 2019 ("Florida Subclass").

95. Excluded from each of the above Classes are Citrix and any of its affiliates, parents or subsidiaries; all employees of Citrix; all persons who make a timely election to be excluded from the Class; government entities; and the judges to whom this case is assigned and their immediate family and court staff.

96. Plaintiff hereby reserves the right to amend or modify the class definition with greater specificity or division after having had an opportunity to conduct discovery.

97. Each of the proposed Classes meets the criteria for certification under Rule 23(a), (b)(2), (b)(3) and (c)(4).

98. **Numerosity. Fed. R. Civ. P. 23(a)(1).** Consistent with Rule 23(a)(1), the members of the Class are so numerous and geographically dispersed that the joinder of all members is impractical. While the exact number of Class members is unknown to Plaintiff at this time, the proposed Class includes potentially tens of thousands of individuals whose Personal Information was compromised in the Data Breach. Class members may be identified through objective means. Class members may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods, which may include U.S. mail, electronic mail, internet postings, and/or published notice.

99. **Commonality. Fed. R. Civ. P. 23(a)(2) and (b)(3).** Consistent with Rule 23(a)(2) and with 23(b)(3)'s predominance requirement, this action involves common questions of law and fact that predominate over any questions affecting individual Class members. The common questions include:

a. Whether Citrix had a duty to protect Personal Information;

b. Whether Citrix knew or should have known of the susceptibility of its systems to a data breach;

c. Whether Citrix's security measures to protect its systems were reasonable in light known legal requirements, such as the FTC data security recommendations, and industry standards;

d. Whether Citrix was negligent in failing to implement reasonable and adequate security procedures and practices;

e. Whether Citrix's failure to implement adequate data security measures allowed the breach of its data systems to occur;

f. Whether Citrix's conduct constituted unfair or deceptive trade practices;

g. Whether Citrix's conduct, including its failure to act, resulted in or was the proximate cause of the breach of its systems, resulting in the loss of the Personal Information of Plaintiff and Class members;

h. Whether Plaintiff and Class members were injured and suffered damages or other losses because of Citrix's failure to reasonably protect its systems and data network; and,

i. Whether Plaintiff and Class members are entitled to relief.

100. **Typicality. Fed. R. Civ. P. 23(a)(3).** Consistent with Rule 23(a)(3), Plaintiff's claims are typical of those of other Class members. Plaintiff is a former employee whose Personal Information was in Citrix's possession at the time of the Data Breach and was compromised as a result of the Data Breach. Plaintiff's damages and injuries are akin to other Class members and Plaintiff seeks relief consistent with the relief of the Class.

101. **Adequacy. Fed. R. Civ. P. 23(a)(4).** Consistent with Rule 23(a)(4), Plaintiff is an adequate representative of the Class because Plaintiff is a member of the Class and is committed to pursuing this matter against Citrix to obtain relief for the Class. Plaintiff has no conflicts of interest with the Class. Plaintiff's Counsel are competent and experienced in litigating class actions, including extensive experience in data breach and privacy litigation. Plaintiff intends to vigorously prosecute this case and will fairly and adequately protect the Class's interests.

102. **Superiority. Fed. R. Civ. P. 23(b)(3).** Consistent with Rule 23(b)(3), a class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The purpose of the class action mechanism is to permit litigation against wrongdoers even when damages to individual plaintiffs may not be sufficient to justify individual litigation. Here, the damages suffered by Plaintiff and the Class are relatively small compared to the burden and expense required to individually litigate their claims against Citrix, and thus, individual litigation to redress Citrix's wrongful conduct would be impracticable. Individual litigation by each Class member would also strain the court system. Individual litigation creates the potential for inconsistent or contradictory judgments, and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economies of scale, and comprehensive supervision by a single court.

103. **Injunctive and Declaratory Relief.** Class certification is also appropriate under Rule 23(b)(2) and (c). Defendant, through its uniform conduct, acted or refused to act on grounds generally applicable to the Class as a whole, making injunctive and declaratory relief appropriate to the Class as a whole.

104. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Citrix owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their Personal Information;

b. Whether Citrix's security measures to protect is systems were reasonable in light of known legal requirements, such as the FTC data security recommendations, and industry standards;

c. Whether Citrix failed to take commercially reasonable steps to safeguard the Personal Information of Plaintiff and the Class members; and,

d. Whether adherence to, FTC data security recommendations, industry standards, and measures recommended by data security experts would have reasonably prevented the Data Breach.

105. Finally, all members of the proposed Class are readily ascertainable. Citrix has access to information regarding which of its employees, former employees, and their beneficiaries and dependents were affected by the Data Breach, the time period of the Data Breach, and which individuals were potentially affected. Using this information, the members of the Class can be identified and their contact information ascertained for purposes of providing notice to the Class.

CAUSES OF ACTION

COUNT I
NEGLIGENCE
(ON BEHALF OF PLAINTIFF AND THE NATIONWIDE CLASS, OR, ALTERNATIVELY, PLAINTIFF AND THE FLORIDA SUBCLASS)

106. Plaintiff restates and re-alleges the preceding paragraphs 1 through 105 as if fully set forth herein.

107. Citrix owed a duty to Plaintiff and the Class to exercise reasonable care in obtaining, securing, safeguarding, storing, and protecting Plaintiff's and Class members' Personal Information within its control from being compromised, lost, stolen, accessed and misused by unauthorized persons. This duty includes, among other things, designing, maintaining and testing Citrix's security systems to ensure that Plaintiff's and Class members' information in Citrix's possession was adequately secured and protected.

108. Citrix owed a duty of care to Plaintiff and members of the Class to provide security, consistent with industry standards, to ensure that its systems and networks adequately protected the Personal Information of its current and former employees.

109. Citrix owed a duty of care to Plaintiff and members of the Class because they were foreseeable and probable victims of any inadequate security practices. Citrix knew or should have known of the inherent risks in collecting and storing the Personal Information of its current and former employees and the critical importance of adequately securing such information.

110. Plaintiff and members of the Class entrusted Citrix with their Personal Information on the premise and with the understanding that Citrix would safeguard their information, and Citrix was in a position to protect against the harm suffered by Plaintiff and members of the Class as a result of the Data Breach.

111. Citrix's own conduct also created a foreseeable risk of harm to Plaintiff and Class members and their Personal Information. Citrix's misconduct included failing to: (1) secure its systems, despite knowing their vulnerabilities, (2) comply with industry standard data security

practices, (3) implement adequate system and event monitoring, and (4) implement the systems, policies, and procedures necessary to prevent this type of data breach.

112. Citrix knew, or should have known, of the risks inherent in collecting and storing Personal Information, the vulnerabilities of its systems, and the importance of adequate security. Citrix knew about numerous, well-publicized data breaches within the technology industry including those targeting its own company.

113. Citrix breached its duties to Plaintiff and Class members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Personal Information of Plaintiff and Class members.

114. Because Citrix knew that a breach of its systems would damage tens of thousands of current and former Citrix employees, including Plaintiff and Class members, Citrix had a duty to adequately protect its data systems and the Personal Information contained thereon.

115. Citrix had a special relationship with Plaintiff and Class members. Plaintiff's and Class members' willingness to entrust Citrix with their Personal Information as a condition of employment was predicated on the understanding that Citrix would take adequate security precautions.

116. Citrix also had independent duties under state and federal laws that required Citrix to reasonably safeguard Plaintiff's and Class members' Personal Information and promptly notify them about the Data Breach.

117. Citrix breached its duties to Plaintiff and Class members in numerous ways, including:

a. by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Personal Information of Plaintiff and Class members;

b. by creating a foreseeable risk of harm through the misconduct previously described;

c. by failing to implement adequate security systems, protocols and practices sufficient to protect Plaintiff's and Class members' Personal Information both before and after learning of the Data Breach;

d. by failing to comply with industry standard data security standards during the period of the Data Breach; and

e. by failing to timely and accurately disclose that Plaintiff's and Class members' Personal Information had been improperly acquired or accessed.

118. The law further imposes an affirmative duty on Citrix to timely disclose the unauthorized access and theft of the Personal Information to Plaintiff and the Class so that Plaintiff and Class members can take appropriate measures to mitigate damages, protect against adverse consequences, and thwart future misuse of their Personal Information.

119. Citrix breached its duty to notify Plaintiff and Class Members of the unauthorized access by waiting to notify Plaintiff and Class members and then by failing to provide Plaintiff and Class members sufficient information regarding the breach including disclosing what information was compromised and who was affected. To date, Citrix has not provided sufficient information to Plaintiff and Class members regarding the extent of the unauthorized access and continues to breach its disclosure obligations to Plaintiff and the Class.

120. Through Citrix's acts and omissions described in this Complaint, including Citrix's failure to provide adequate security and its failure to protect Personal Information of Plaintiff and Class members from being foreseeably captured, accessed, disseminated, stolen and misused, Citrix unlawfully breached its duty to use reasonable care to adequately protect and secure Personal Information of Plaintiff and Class members during the time it was within Citrix's possession or control.

121. Further, through its failure to provide timely and clear notification of the Data Breach to consumers, Citrix prevented Plaintiff and Class members from taking meaningful, proactive, and targeted measures to mitigate against potential harm.

122. Citrix improperly and inadequately safeguarded the Personal Information of Plaintiff and Class members in deviation of standard industry rules, regulations, and practices at the time of the unauthorized access. Citrix's failure to take proper security measures to protect sensitive Personal Information of Plaintiff and Class members as described in this Complaint, created conditions conducive to a foreseeable, intentional criminal act, namely the unauthorized access of Personal Information of Plaintiff and Class members.

123. Citrix's conduct was grossly negligent and departed from all reasonable standards of care, including, but not limited to: failing to adequately protect the Personal Information; failing to conduct regular security audits; failing to provide adequate and appropriate supervision of persons having access to Personal Information of Plaintiff and Class members; and failing to provide Plaintiff and Class members with timely and sufficient notice that their sensitive Personal Information had been compromised.

124. Neither Plaintiff nor the other Class members contributed to the Data Breach and subsequent misuse of their Personal Information as described in this Complaint.

125. As a direct and proximate cause of Citrix's conduct, Plaintiff and the Class suffered damages including, but not limited to: damages arising from the unauthorized charges on their debit or credit cards or on cards that were fraudulently obtained through the use of the Personal Information of Plaintiff and Class members; damages arising from identity theft or fraud; damages from lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives including, inter alia, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports and damages from identity theft, which may take months if not years to discover and detect, given the far-reaching, adverse and detrimental consequences of identity theft and loss of privacy. The nature of other forms of economic damage and injury may take years to detect, and the potential scope can only be assessed after a thorough investigation of the facts and events surrounding the theft mentioned above.

COUNT II
NEGLIGENCE PER SE
(ON BEHALF OF PLAINTIFF AND THE NATIONWIDE CLASS, OR, ALTERNATIVELY, PLAINTIFF AND THE FLORIDA SUBCLASS)

126. Plaintiff restates and re-alleges the preceding paragraphs 1 through 105 as if fully set forth herein.

127. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Citrix, of failing to use reasonable measures to protect Personal Information. 15 U.S.C. § 45(a)(1).

128. The FTC publications and orders described above also form part of the basis of Citrix's duty in this regard.

129. Citrix violated Section 5 of the FTC Act by failing to use reasonable measures to protect Personal Information and not complying with applicable industry standards, as described in detail herein. Citrix's conduct was particularly unreasonable given the nature and amount of Personal Information it obtained and stored, and the foreseeable consequences of a data breach at a company as large as Citrix, including, specifically, the immense damages that would result to Plaintiff and Class members.

130. Citrix's violation of Section 5 of the FTC Act constitutes negligence *per se*.

131. Plaintiff and Class members are within the class of persons that the FTC Act was intended to protect.

132. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

133. Moreover, Florida law requires that covered entities "take reasonable measures to protect and secure data in electronic form containing personal information." Fla. Stat. § 501.171(2).

134. "Covered entity" in includes any "commercial entity that acquires, maintains, stores, or uses personal information." Fla. Stat. § 501.171(1)(b).

135. "Personal information" means "[a]n individual's first name or first initial and last name in combination with" several additional data elements for that individual, including, social security number; driver license or identification card number; and/or financial account number or credit or debit card number. Fla. Stat. § 501.171(1)(g).

136. Citrix violated section 501.171(2) by failing to take reasonable measures to protect and secure Plaintiff's and Class Member's Personal Information.

137. The harm that occurred as a result of the Data Breach is the type of harm section 501.171(2) was intended to guard against, and Plaintiff and the Class are in the class of persons the section was intended to protect.

138. As a direct and proximate result of Citrix's negligence *per se*, Plaintiff and the Class have suffered, and continue to suffer, injuries damages arising from identity theft or fraud; damages from lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives including, inter alia, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports and damages from identity theft, which may take months if not years to discover and detect, given the far-reaching, adverse and detrimental consequences of identity theft and loss of privacy.

COUNT III
VIOLATIONS OF THE OF THE FLORIDA UNFAIR AND DECEPTIVE TRADE PRACTICES ACT, FLA. STAT. §§ 501.201, *et seq.*

(ON BEHALF OF PLAINTIFF AND THE NATIONWIDE CLASS, OR, ALTERNATIVELY, PLAINTIFF AND THE FLORIDA SUBCLASS)

139. Plaintiff restates and re-alleges the preceding paragraphs 1 through 105 as if fully set forth herein.

140. Citrix engaged in the conduct alleged in this Complaint through transactions in and involving trade and commerce. Mainly, the Data Breach occurred through the use of the internet, an instrumentality of interstate commerce.

141. As alleged herein this Complaint, Citrix engaged in unfair or deceptive acts or practices in the conduct of consumer transactions, including, among other things, the following:

a. failure to implement data adequate security practices to safeguard Personal Information;

b. failure to make only authorized disclosures of employees' Personal Information; and

c. failure to timely and accurately disclose the Data Breach to Plaintiff and Class members.

d. failure to disclose that its computer systems and data security practices were inadequate to safeguard Personal Information from theft; and

e. failure to timely and accurately disclose the Data Breach to Plaintiff and Class members;

142. These unfair acts and practices violated duties imposed by laws including by not limited to Section 5 of the FTC Act and Fla. Stat. § 501.171(2).

143. Citrix's actions constitute unconscionable, deceptive, or unfair acts or practices because, as alleged herein, Citrix engaged in immoral, unethical, oppressive, and unscrupulous activities that are and were substantially injurious to its current and former employees.

144. In committing the acts alleged above, Citrix engaged in unconscionable, deceptive, and unfair acts and practices acts by omitting, failing to disclose, or inadequately disclosing to its current and former employees that it did not follow industry best practices for the collection, use, and storage of Personal Information.

145. As a direct and proximate result of Citrix's conduct, Plaintiff and other members of the Class have been harmed and have suffered damages including, but not limited to: damages arising from identity theft and fraud; current and future out-of-pocket costs in connection with preparing and filing tax returns; out-of-pocket expenses associated with procuring identity protection and restoration services; increased risk of future identity theft and fraud, and the costs associated therewith; and time spent monitoring, addressing and correcting the current and future consequences of the Data Breach.

146. As a direct and proximate result of the unconscionable, unfair, and deceptive acts or practices alleged herein, Plaintiff has been damaged and is entitled to recover actual damages, declaratory and injunctive relief, and reasonable attorneys' fees and costs, to the extent permitted by law.

147. Also as a direct result of Citrix's knowing violation of the Florida Unfair and Deceptive Trade Practices Act, Plaintiff and Class members are entitled to damages as well as injunctive relief, including, but not limited to:

A. Ordering that Citrix engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Citrix's systems on a periodic basis, and ordering Citrix to promptly correct any problems or issues detected by such third-party security auditors;

B. Ordering that Citrix engage third-party security auditors and internal personnel to run automated security monitoring;

C. Ordering that Citrix audit, test, and train its security personnel regarding any new or modified procedures;

D. Ordering that Citrix segment Personal Information by, among other things, creating firewalls and access controls so that if one area of Citrix is compromised, hackers cannot gain access to other portions of Citrix systems;

E. Ordering that Citrix purge, delete, and destroy in a reasonable secure manner Personal Information not necessary for its provisions of services;

F. Ordering that Citrix conduct regular database scanning and securing checks;

G. Ordering that Citrix routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

H. Ordering Citrix to meaningfully educate its employees about the threats they face as a result of the loss of their Personal Information to third parties, as well as the steps Citrix employees must take to protect themselves.

COUNT IV
BREACH OF IMPLIED CONTRACT

(ON BEHALF OF PLAINTIFF AND THE NATIONWIDE CLASS, OR, ALTERNATIVELY, PLAINTIFF AND THE FLORIDA SUBCLASS)

148. Plaintiff restates and re-alleges the preceding paragraphs 1 through 105 as if fully set forth herein.

149. Plaintiff and Class members were required to provide their Personal Information, including names, addresses, Social Security numbers, financial information, and other personal information, to Citrix as a condition of their employment.

150. Implicit in the employment agreement between the Citrix and its employees was the obligation that Citrix would use the Personal Information of its employees for business purposes only and not make unauthorized disclosures of the information.

151. Citrix had an implied duty to reasonably safeguard and protect the Personal Information of Plaintiff and Class members from unauthorized disclosure or uses.

152. Additionally, Citrix implicitly promised to retain this Personal Information only under conditions that kept such information secure and confidential.

153. Plaintiff and Class members fully performed their obligations under the implied contract with Citrix. Citrix did not.

154. Citrix breached the implied contracts with Plaintiff and Class members by failing to reasonably safeguard and protect Plaintiff' and Class members' Personal Information, which was compromised as a result of the Data Breach.

155. Citrix's acts and omissions have materially affected the intended purpose of the implied contacts requiring Plaintiff and Class members to provide their Personal Information as a condition of employment in exchange for compensation and benefits.

156. As a direct and proximate result of Citrix breach of its implied contacts with Plaintiff and Class members, Plaintiff and Class members have suffered and will suffer injury, including but not limited to: (i) the loss of the opportunity how their Personal Information is used; (ii) the compromise, publication, and/or theft of their Personal Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Personal Information; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from tax fraud and identity theft; (v) costs associated with placing freezes on credit reports; (vi) the continued risk to their Personal Information, which remains in Citrix possession and is subject to further unauthorized disclosures so long as Citrix fails to undertake appropriate and adequate measures to protect the Personal Information of employees and former employees in its continued possession; and, (vii) future costs in terms of time, effort and money that will be expended to prevent, detect, contest, and repair the impact of the Personal Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class members.

COUNT V
BREACH OF FIDUCIARY DUTY
(ON BEHALF OF PLAINTIFF AND THE NATIONWIDE CLASS, OR, ALTERNATIVELY, PLAINTIFF AND THE SEPARATE FLORIDA SUBCLASS)

157. Plaintiff restates and re-alleges the preceding paragraphs 1 through 105 as if fully set forth herein.

158. In light of the special relationship between Citrix and its employees, whereby Citrix required Plaintiff and Class Members to provide highly sensitive, confidential, personal and

financial information as a condition of their employment, Citrix was a fiduciary, as an employer created by its undertaking, to act primarily for the benefit of its employees, including Plaintiff and Class members, for the safeguarding of employees' Personal Information.

159. Citrix had a fiduciary duty to act for the benefit of Plaintiff and Class members upon matters within the scope of their employer/employee relationship, in particular to keep secure the Personal Information of its current and former employees.

160. Citrix breached its duty of care to Plaintiff and Class members to ensure that their Personal Information was not disclosed without authorization or used for improper purposes by failing to provide adequate protections to the information and by disclosing the information to an unknown and unauthorized third party.

161. As a direct and proximate result of the Citrix actions alleged above, Plaintiff and Class members have suffered actual damages as alleged herein.

COUNT VI
BREACH OF CONFIDENCE
(ON BEHALF OF PLAINTIFF AND THE NATIONWIDE CLASS, OR, ALTERNATIVELY, PLAINTIFF AND THE FLORIDA SUBCLASS)

162. Plaintiff restates and re-alleges the preceding paragraphs 1 through 105 as if fully set forth herein.

163. At all times during Plaintiff's and Class Members' interactions with Defendant, Defendant was fully aware of the confidential and sensitive nature of Plaintiff's and Class Members' Personal Information that Plaintiff and Class Members provided to Defendant.

164. As alleged herein and above, Defendant's relationship with Plaintiff and Class' Members was governed by expectations that Plaintiff's and Class Members' Personal Information

would be collected, stored, and protected in confidence, and would not be disclosed to unauthorized third parties.

165. Plaintiff and Class Members provided their respective Personal Information to Defendant with the explicit and implicit understandings that Defendant would protect and not permit their sensitive Personal Information to be disseminated to any unauthorized parties.

166. Plaintiff and Class Members also provided their respective Personal Information to Defendant with the explicit and implicit understanding that Defendant would take precautions to protect that Personal Information from unauthorized disclosure, such as following basic principles of information security practices.

167. Defendant voluntarily received in confidence Plaintiff's and Class Members' Personal Information with the understanding that the Personal Information would not be disclosed or disseminated to the public or any unauthorized third parties.

168. Due to Defendant's failure to prevent, detect, and/or avoid the Data Breach from occurring by, inter alia, failing to follow best information security practices to secure Plaintiff's and Class Members' Personal Information, Plaintiff's and Class Members' Personal Information was disclosed and misappropriated to unauthorized third parties beyond Plaintiff's and Class Members' confidence, and without their express permission.

169. As a direct and proximate cause of Defendant's actions and/or omissions, Plaintiff and Class Members have suffered damages as alleged herein.

170. But for Defendant's disclosure of Plaintiff's and Class Members' Personal Information in violation of the parties' understanding of confidence, their Personal Information would not have been compromised, stolen, viewed, accessed, and used by unauthorized third

parties. Defendant's Data Breach was the direct and legal cause of the theft of Plaintiff's and Class Members' Personal Information, as well as the resulting damages.

171. The injuries and harm Plaintiff and Class Members suffered were the reasonably foreseeable result of Defendant's unauthorized disclosure of Plaintiff's and Class Members' Personal Information. Defendant knew its computer systems and technologies for accepting and securing Plaintiff's and Class Members' Personal Information had security vulnerabilities because Defendant failed to observe industry standard information security practices.

172. As a direct and proximate result of Defendant's breaches of confidence, Plaintiff and the Class have suffered, and continue to suffer, injuries and damages arising from identity theft; Plaintiff's inability to use their debit or credit cards because those cards were cancelled, suspended, or otherwise rendered unusable as a result of the Data Breach and/or false or fraudulent charges stemming from the Data Breach, including but not limited to late fees charged and foregone cash back rewards; damages from lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives, including, inter alia, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports, and damages from identity theft, which may take months if not years to discover and detect, given the far-reaching, adverse and detrimental consequences of identity theft and loss of privacy

173. As a direct and proximate result of Defendant's breaches of confidence, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm,

including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses as set forth herein.

COUNT VII
DECLARATORY JUDGMENT
(ON BEHALF OF PLAINTIFF AND THE NATIONWIDE CLASS, OR, ALTERNATIVELY, PLAINTIFF AND THE FLORIDA SUBCLASS)

174. Plaintiff restates and re-alleges the preceding paragraphs 1 through 105 as if fully set forth herein.

175. As previously alleged, Plaintiff and Class members entered into an implied contract that required Citrix to provide adequate security for the Personal Information it collected from them. As previously alleged, Citrix owes duties of care to Plaintiff and Class members that require it to adequately secure Personal Information.

176. Citrix still possesses Personal Information pertaining to Plaintiff and Class members.

177. Citrix has made no announcement or notification that it has remedied the vulnerabilities in its computer data systems.

178. Accordingly, Citrix has not satisfied its contractual obligations and legal duties to Plaintiff and Class members. In fact, now that Citrix's lax approach towards data security has become public, the Personal Information in its possession is more vulnerable than it was prior to announcement of the Data Breach.

179. Actual harm has arisen in the wake of the Data Breach regarding Citrix's contractual obligations and duties of care to provide data security measures to Plaintiff and Class members.

180. Plaintiff, therefore, seeks a declaration that (a) Citrix's existing data security measures do not comply with its contractual obligations and duties of care, and (b) in order to comply with its contractual obligations and duties of care, Citrix must implement and maintain reasonable security measures, including, but not limited to:

a. engaging third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Citrix's systems on a periodic basis, and ordering Citrix to promptly correct any problems or issues detected by such third-party security auditors;

b. engaging third-party security auditors and internal personnel to run automated security monitoring;

c. auditing, testing, and training its security personnel regarding any new or modified procedures;

d. segmenting Personal Information by, among other things, creating firewalls and access controls so that if one area of Citrix is compromised, hackers cannot gain access to other portions of Citrix systems;

e. purging, deleting, and destroying in a reasonable secure manner Personal Information not necessary for its provisions of services;

f. conducting regular database scanning and securing checks;

g. routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

h. educating its customers about the threats they face as a result of the loss of their financial and personal information to third parties, as well as the steps Citrix customers must take to protect themselves.

REQUEST FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of all Class members proposed in this Complaint, respectfully request that the Court enter judgment in her favor and against Citrix as follows:

a. For an Order certifying the Classes, as defined herein, and appointing Plaintiff and her Counsel to represent the Nationwide Class, or in the alternative the separate Florida Subclass;

b. For equitable relief enjoining Citrix from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class members' Personal Information, and from refusing to issue prompt, complete and accurate disclosures to the Plaintiff and Class members;

c. For equitable relief compelling Citrix to use appropriate cyber security methods and policies with respect to consumer data collection, storage and protection and to disclose with specificity to Class members the type of Personal Information compromised;

d. For an award of damages, including nominal damages, as allowed by law in an amount to be determined;

e. For an award of attorneys' fees costs and litigation expenses, as allowable by law;

f. For prejudgment interest on all amounts awarded; and

g. Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMAND

Plaintiff demands a jury trial on all issues so triable.

Friday, May 24, 2019.

/s/ John A. Yanchunis
JOHN A. YANCHUNIS
Florida Bar No. 324681
jyanchunis@ForThePeople.com
PATRICK A. BARTHLE II
Florida Bar No. 99286
pbarthle@ForThePeople.com
MORGAN & MORGAN
COMPLEX LITIGATION GROUP
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
Telephone: (813) 223-5505
Facsimile: (813) 223-5402

Norman E. Siegel (*Pro hac vice* to be submitted)
Barrett J. Vahle (*Pro hac vice* to be submitted)
J. Austin Moore (*Pro hac vice* to be submitted)
STUEVE SIEGEL HANSON LLP
460 Nichols Road, Suite 200
Kansas City, Missouri 64112
Tel: (816) 714-7100
Fax: (816) 714-7101
siegel@stuevesiegel.com
vahle@stuevesiegel.com
moore@stuevesiegel.com

Attorneys for Plaintiff and Proposed Classes